Ethical hacking lab: Support HackTheBox

"Mi intención, además de llevar un Conteo y Evidencia de mi progreso en la formación como Pentester, es despertar la curiosidad en la comunidad mexicana y de habla hispana sobre temas de Hacking Ético. Quiero ofrecer lo que considero una explicación 'sencilla' de lo complejo y fascinante que son los sistemas vulnerables en la actualidad."

/▲\ Correo /▲\ tiktok /▲\ github

Atacante ---------- |10.10.19.30|

|>/////////// Linux|

Victima ---------- |10.10.11.130|

|> /////// Windows|

Walkthrough

Iniciamos validando el alcance con un ping. El valor del TTL es 63, lo que nos sugiere que posiblemente nos enfrentamos a un entorno Linux. Lo siguiente es enumerar sus puertos y servicios, encontrando el puerto 22 con SSH en su versión 7.6 y el puerto 80 con un servicio HTTP.

La herramienta WhatWeb nos ayuda a listar las tecnologías utilizadas en su servicio web, pero nos arroja un redireccionamiento a horizontall.htb, el cual añadiremos a nuestro archivo **/etc/hosts**. Al establecer esto, podemos visualizar que el entorno utiliza un gestor de contenido llamado Strapi, basado en Node.js.

Con un ataque de fuerza bruta, la ayuda de un diccionario y la herramienta Wfuzz, podemos descubrir rutas de la página web que no deberíamos ver, ya que en este caso hay una fuga de información que revela un subdominio. Este subdominio lo volveremos a atacar con fuerza bruta para descubrir una ruta "guionadmin", que revela que se está desplegando la versión 3.0 de Strapi.

Antes de continuar, es importante mencionar que existe una base de datos que recopila vulnerabilidades y exploits de herramientas y sistemas conocidos llamada Exploit Database, registrada con las siglas CVE (Common Vulnerabilities and Exposures), que incluye el año en el que se hizo pública la vulnerabilidad, un número identificador y su extensión.

En este caso, hay un registro de una vulnerabilidad de tipo ejecución remota de comandos sin autenticar, siendo un script en Python, que sigue los siguientes pasos:

1. Verificar la versión de Strapi.
2. Restablecer la contraseña de administrador explotando una vulnerabilidad en la validación de códigos, que permite cambiar la contraseña sin autorización.
3. Obtener el JSON Web Token tras el restablecimiento exitoso de la contraseña.
4. Abusar del JSON Web Token para brindarnos una consola medianamente funcional.

Aprovechamos esa ejecución de comandos para establecer una shell inversa utilizando las funciones curl y bash, ejecutando código alojado en un servicio HTTP local con Python.

Ya como el usuario "strapi" del equipo de la víctima, tenemos permisos de visualización a la primera flag de las dos que nos pide la plataforma para validar que efectivamente vulneramos el sistema. Estas banderas son únicas para cada jugador.

Enumerando el sistema, vemos que podemos ejecutar en la máquina el comando pkexec, del cual es posible abusar para escalar nuestro privilegio a administrador, ya que esta herramienta controla privilegios a nivel de sistema. Finalmente, encontramos la segunda flag del entorno, siendo esta la del usuario root.